Paula Seles, Esq.
Senior Counsel
Washington Attorney General's Office
900 4th Avenue, Suite 2000
Seattle, WA 98164

Dear Paula:

Thank you for the opportunity to comment on the Attorney Generals' recent report on "Consumer Privacy Protection and Commercial Best Practices." These comments will serve to supplement comments to the "Best Practices" section of the report that were submitted on January 30th.

The report is a good first step at educating consumers and policy makers regarding the various issues surrounding privacy law and information sharing practices. We would suggest however, that the report be revised to reflect the progress that industry has made in providing consumers with technological solutions to controlling the collection and dissemination of their information online. Further, the report also draws several conclusions regarding governmental attempts to regulate information collection practices, as well as interpretations of consumer activity online that are not well-supported or documented by the evidence contained in the report. In addition, the report should consider private and public reports and surveys that contain information and arguments that are contrary to the conclusions reached by the report.

I. Introduction

The report begins by noting that "regulations are not sufficient, by themselves, to protect consumers," that "businesses clearly have a vested interest in assuring that privacy issues are addressed through new legislation or self-regulated privacy policies," and that while "The federal government has created a number of laws addressing the rights of individuals with respect to the government's use of personal information. . . there are relatively few laws governing the use of personal information by private entities."

We disagree that current regulations, by themselves, are not sufficient to protect consumers. As the report notes, the US has taken a sectoral approach to privacy regulation. As such, information collection practices are currently regulated across the financial, health care, cable and telecommunications industries and there is no indication that these statutes have failed to provide consumers with adequate privacy protection.

Furthermore, since 1999 the Federal Trade Commission (FTC) has conducted or supported a "web sweep" to assess the progress made by industry to adopt and provide notice of their online privacy policies. While each web sweep has been slightly different, in general the FTC has examined (1) a random sample of sites to get a sense of the overall adoption rate of privacy policies and (2) the most 100 most-visited commercial sites that account for roughly 95% of all web traffic. The FTC's 2000 report found that all of the most-visited sites offer notice of their information practices. This means that roughly 95% or more of all commercial Internet traffic is conducted over sites that disclose their information practices and are therefore subject to the deceptive trade practice authority of the FTC and state attorneys general.

Further, while it might be accurate to say that business would like to see privacy issues addressed through self-regulated privacy policies, there is no consensus within the industry that privacy should be handled through new legislation. Most companies, including Microsoft,

oppose privacy legislation and additional regulatory requirements, especially given the recent downturn in the national economy and the decline in the online industry and "dot.com" sectors.

Finally, one could infer from the statement regarding "government laws" versus "private sector" laws that the government is doing more than private industry to protect the privacy of personal information that they collect. While we are sure that is not the message the report intended to send, there should be language providing background with regard to private sector initiatives such as P3P, third party seal programs, anonymizer technologies and other tools that offer users the ability to control their personal information.

II. Consumer Concerns About Privacy

The report cites identity theft and telemarketing fraud as examples of "byproducts of the proliferation and free flow of information" and that the incidence of each can be "correlated to the loss of privacy," and the result of the "free availability of personal information that enhances the ability of fraudulent telemarketers to victimize consumers." But it is not necessarily true that identity theft is a byproduct of information sharing. The most effective way to make identity theft difficult is not to try to bottle up personal information, but rather to develop and institute stronger methods of authenticating identity, i.e. smart cards.

In its most common form, identity theft occurs when criminals illegally obtain a consumer's personal information (i.e. bank and credit card account number, phone number, PIN, social security number) in order to illegally obtain credit, charge goods in the name of the victim, or electronically divert funds from the victim's bank account. Identity theft requires no direct communication or contact between criminal and victim. Indeed, the most common forms of identity theft usually take place in the course of everyday transactions – charging dinner at a restaurant, submitting required personal information to employers or government agencies, throwing away catalogs received in the mail, or through casual contact and conversation. Any of these scenarios could give identity thieves an opportunity to obtain unauthorized access to personal information.

Another effective way to combat identity theft is to educate consumers and policy makers as to the root causes of identity theft and by encouraging consumers to minimize their risk by managing personal information wisely, cautiously and with heightened sensitivity. For example, in its report "*ID Theft, When Bad Things Happen to Your Good Name,*" the FTC has identified several steps that consumers can take to minimize the risk of identity theft including: 1) finding out how personal information will be used or shared (including whether such information can be kept confidential) before revealing such information with vendors; 2) follow up with creditors if bills don't arrive on time (missing credit card bills could mean that a criminal has accessed an account and changed the mailing address); 3) put holds on mail delivery during vacation; 4) place passwords on credit card, bank and phone accounts; 5) limit disclosure of personal information on the phone or over the Internet unless the customer has initiated the call or knows who they're dealing with; 6) give out social security numbers only when necessary; 7) order a copy of your credit report every year from each of the three major credit reporting agencies.

With regard to telemarketing fraud, the report recites the "BrandDirect Marketing" case to describe the practice of using pre-acquired account telemarketing information to make unauthorized charges on the customer's credit card accounts. However, the kind of account information sharing described in the paper is now prohibited by section 313.12 of the Gramm-Leach Bliley Act, and the telemarketing fraud activity described in this case took place before GLB's effective. Given that this problem has been addressed by Congress, reciting this scenario

in the report without the proper background gives the reader the impression that such activity is legal, has been left unaddressed and that victims are currently without recourse.

In the discussion of "Online Data Collection" the Report also uses a Gallup Poll and the 2000 FTC report to support its conclusion that consumers are clearly concerned about how their private PII and financial information is being used. Further, the report cites the FTC's Report for the conclusion that that 97-99% of web sites collect at least one type of personal information from site visitors and that 92% collect PI such as SS#, gender and age.

Aside from the selective use of the FTC's data (i.e. failing to note that 95% of all commercial Internet traffic is subject to FTC and state AG enforcement authority), there is no distinction made between personally identifiable information and demographic data. Age and gender are not considered particularly worrisome pieces of data, even by the most ardent privacy hawks and should not be placed in the same category as social security numbers. Further, the statement seems to indicate that 92% of web sites collect social security numbers. We do not believe this to be the case and have not seen empirical data supporting this assertion.

III. Information Gathering Practices

This section pays a good amount of attention to online information gathering practices and the use of cookies, clickstream data and online profiling. However, for the reasons articulated below, the report could provide a more complete picture of how cookies collect information, how they are used, and industry efforts to provide consumers with tools to regulate the use and placement of cookies.

The section begins by discussing how the infrastructure of the Internet permits computer systems operators to capture and store online data of any sites on the Internet that the user visits and that it is apparent that privacy concerns stem from technological parameters. The report cites to a footnote discussing the TCP/IP protocol as support for this conclusion.

As an initial point, it is true that TCP/IP has become the most widely accepted networking protocol and permits wide information sharing on the connected Internet. However there is no statement to make the link that the TCP/IP protocol is in anyway related to monitoring concerns. Moreover, there is no attempt to test this hypothesis against the specific statements by ISPs indicating that they do not engage in such monitoring.

The second heading in section B, "Cookies, Clickstream Data and the *Perils* (emphasis added) of Online Profiling," seems to imply that there are no legitimate benefits of online profiling. Given the fact that the section points out some of the benefits of online profiling (targeted advertising) and notes that such practices are routinely used in the offline world, the title should be changed to give the appearance of a more balanced consideration of this issue.

Furthermore, the section categorizes network advertisers as "uninvited guests," to the user's online experience. This mischaracterizes the nature of these companies. Network advertisers are invited by the website on which the banner ads appear. To use a real-world example, if I visited your house, and you have invited another person there as well, I would not call that person an "uninvited guest" even if I did not expect to see that person. It's your house and you can invite whomever you want. Likewise, if I visit your website, it's not up to me to decide who is invited and who is uninvited.

The report also focuses on the online profiling practices of third party ad server companies such as DoubleClick. Specifically, that while cookies do not gather data, companies

such as Double Click use cookies as tracking devices. This information is gathered, and associated with a value that is kept in the user's cookie, to create a "clickstream" of data which shows the history of the user's presence on various websites. While the report correctly notes that a cookie cannot read a hard drive for personal information (in so far as companies such as Double Click anonymously track behavior across multiple sites) the report states that a site can put PII in a cookie if the user provides it to a site.

This is not true and confuses the concepts of using profiles derived from cookies and merging them with PII. If a user provides PII to a site, that PII can be stored in the cookie by that site, but it would not be stored in the cookie set by the third party ad provider. From the perspective of the third party ad provider, the user is still anonymous. Further, such profiles (cookie data merged with PII) can only occur if the user identifies her to the entity creating the profile. These third party ad servers can try various means to try and get the user to identify themselves, (i.e. sweepstakes or contest), but it cannot easily be done without some action on the users' part.

In its discussion of the merging of clickstream and PII, the report references the case of the Double Click-Abacus Direct merger and states that the merger gave Abacus Direct the capacity to "link its own data with Abacus' list of names and purchase histories of 88 million households." However, by acquiring Abacus, Double Click did not automatically gain the capacity to link its anonymous online profiles with the offline PII. Double Click would have had to use various means of getting online users to identify themselves in order to permit the linkage to occur.

This section closes with Double Click's recent announcement that it would suspend any plan to link anonymous data with the individual consumer's name, until a set of common privacy standards were developed. Missing from the report is the fact that in August 2000, the FTC issued a report endorsing the National Advertising Institute's self-regulatory initiative for online profiling. (*See http:www.ftc.gov/os/2000/07.onlineprofiling.htm)*

Finally we feel that there should be some recognition of the numerous efforts that industry has made to empower consumers to limit the prevalence of cookies on their web site. For example, companies such as Microsoft have adopted P3P and built this cookie management technology into the IE6 browser. The report should include a discussion of how P3P is being used to empower consumers to control their online experience.

IV. Regulatory Measures

This section begins by noting the Constitutional issues surrounding the right to privacy in general and with specific regard to information sharing. It then proceeds to note that "the United States does not have a comprehensive privacy statute that governs the collection and use of personally identifiable information, either online or through traditional business practices." Some however, would argue that this is actually beneficial to online commerce and that the enactments of broader bills are premature or inefficient.

But there are no citations or references in the report to the plethora of literature advocating this position. Many of these arguments are based on the Constitutional infirmities that such legislation would raise,[1] and the cost of such legislation and regulation to online commerce.[2]

---

[1] *See,* "Constitutional Issues in Information Privacy" Fred Cate and Robert E. Litan, AEI-Brooking Joint Center for Regulatory Studies, Working Paper 01-11, September 2001; http://www.aei.brookings.org/publications/working/working_01_11.pdf

Even if the report's conclusions differ with these positions, it should at least cite competing viewpoints.

While the report notes that the US has taken a sectoral approach to online privacy protection, its review of recent federal law doesn't portray a broad interpretation of such laws on online privacy and consumer behavior.

In its discussion on Gramm-Leach-Bliley, the report states that the opt-out provision of GLB "has failed" given the fact that only "5 percent nationwide responded to the privacy "opt-out" notices." The report's conclusion begs the question, what percentage of people opting-out would be considered a "success?" If 5 percent is bad, presumably 30 percent would be better and 100 percent would be best. This demonstrates a clear bias in favor of eliminating data sharing altogether.

The report seems to suggest the reason why so few people have decided to "opt-out" of having their information shared with third parties is due to the complexity or legalese of the privacy notice. However, the only basis the report uses for that conclusion is the opinion of a single Seattle Times reporter. There seems to be little consideration of the possibility that consumers are perfectly willing to receive benefits in exchange for the sharing of their information. Or perhaps, that actual consumer behavior does not comport with the gravity of the information sharing problem as it would be characterized by the media or consumer advocates.

Further, the report includes the Communications Assistance for Law Enforcement Act (CALEA) of 1994 (47 USC §§1001-1-10; §1021; 18 USC §2522) in its discussion of current government privacy regulations. It is curious that the report would include CALEA in its discussion of "pro-privacy" laws, as the purpose of CALEA is to enable the ***government*** to listen in on wireless telephone conversations. In fact, CALEA arguably places the government in the unenviable position of intruding on consumer's privacy, as opposed to the various measures that the private sector is currently taking to protect consumer privacy in the online world.

Thank you for your consideration and we look forward to working with the Attorney General's office to discuss these issues in greater detail.

Bill Ashworth
Policy Counsel
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
425-707-6277

---

[2] *See,* "The Benefits and Costs Of Online Privacy Legislation" Robert W. Hahn and Anne Layne-Farrar AEI-Brookings Joint Center for Regulatory Studies, Working Paper 01-14, October 2001; http://papers.ssrn.com/paper.taf?abstract_id=292649; "Where Everybody Knows Your Name: A Pragmatic Look at the Costs of Privacy and the Benefits of Information Exchange," Kent Walker, General Counsel, Liberate Technologies, 2000 Stanford Tech. T. Rev. 1 (December 2000); http://stlr.stanford.edu/STLR/Articles/00_STLR_2